

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AT05/000111

International filing date: 31 March 2005 (31.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: AT
Number: A 573/2004
Filing date: 31 March 2004 (31.03.2004)

Date of receipt at the International Bureau: 29 April 2005 (29.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



PCT/AT 2005/000111

ÖSTERREICHISCHES PATENTAMT

A-1200 Wien, Dresdner Straße 87

Kanzleigebühr € 10,00
Schriftengebühr € 52,00

Aktenzeichen A 573/2004

Das Österreichische Patentamt bestätigt, dass

Dipl.-Ing. Helmut Schluderbacher
in A-1100 Wien, Karmarschgasse 18A/2/11,

am **31. März 2004** eine Patentanmeldung betreffend

"Personenunabhängige Zugangskontrolle",

überreicht hat und dass die beigeheftete Beschreibung samt Zeichnungen mit der ursprünglichen, zugleich mit dieser Patentanmeldung überreichten Beschreibung samt Zeichnungen übereinstimmt.

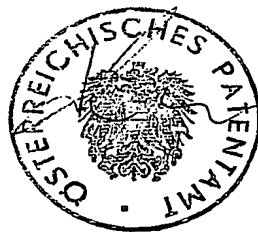
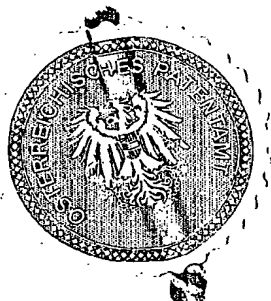
Es wurde beantragt, Dipl.-Ing. Helmut Schluderbacher in Wien, als Erfinder zu nennen.

Österreichisches Patentamt

Wien, am 6. April 2005

Der Präsident:

i. A.



HRNCIR
Fachoberinspektor

A 573/200 4

00000000000000000000
(51) IPC:

Urtext

AT PATENTSCHRIFT

(11) Nr.

(Bei der Anmeldung sind nur die eingerahmten Felder auszufüllen - bitte fett umrandete Felder unbedingt ausfüllen!)

(73)	Patentanmelder (bzw. -inhaber): <i>Dipl.-Ing. Helmut Schluderbacher</i>
(54)	Titel der Anmeldung: <i>Personenunabhängige Zugangskontrolle</i>
(61)	Zusatz zu Patent Nr.
(66)	Umwandlung von <i>GM</i> /
(62)	gesonderte Anmeldung aus (Teilung): <i>A</i> /
(30)	Priorität(en):
(72)	Erfinder: <i>Helmut Schluderbacher</i>

(22) (21) Anmeldetag, Aktenzeichen:

, A /

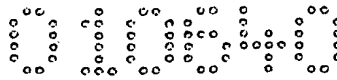
(60) Abhängigkeit:

(42) Beginn der Patentdauer:

Längste mögliche Dauer:

(45) Ausgabetag:

(56) Entgegenhaltungen, die für die Beurteilung der Patentierbarkeit in Betracht gezogen wurden:



Personenunabhängige Zugangskontrolle

1 Patentansprüche / Schutzbegehren

Patentanspruch 1: Verfahren eines graphischen Authentifizierungscodes in welchem sich ein Anwender in einem Zutrittsverfahren an ein technisches System anmeldet **dadurch gekennzeichnet**, dass für den Anwender von dem System Bildschirmfolgen erzeugt werden, dabei werden jeweils eine Menge von Grafiken (Bilder, Symbole, alphanumerische Zeichen und ähnliches) mit zumindest zwei unterschiedlichen Einheiten (Sets) zusammengestellt und angezeigt, über eine geeignete Möglichkeit ermittelt der Anwender zu den Bildschirmfolgen, durch einen ihm bekannten Code bestehend aus alphanumerischen Zeichen, Bildern, Symbolen oder ähnliches, mit Informationen aus zumindest zwei Einheit genau die Informationen, welche einzugeben sind, wobei es dabei keinen direkten Zusammenhang gibt zwischen einer einzelnen Grafik und den zu drückenden Tasten.

Patentanspruch 2: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1 **dadurch gekennzeichnet**, dass die Information welche durch einen Tastendruck erzeugt wird, beliebiger Form ist (graphisch, alphanumerisch oder ähnliches), keine räumliche Information über einzelne Grafiken oder Einheiten am Bildschirm enthält, aus den Bildschirmfolgen gemeinsam mit dem Code des Anwenders (Anwender-Code), eindeutig genau eine Tastenfolge (Antwort-Code) erzeugt und diese genau die ist, welche das System von diesem Anwender erwartet.

Patentanspruch 3: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1 und 2 **dadurch gekennzeichnet**, dass der Anwender seinen Code nicht bei einem anderen System eingeben kann, wenn dieses andere System keine geeigneten Bildschirmfolgen aufbereitet.

Patentanspruch 4: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1 und 2 **dadurch gekennzeichnet**, dass für je zwei aufeinanderfolgende Anmeldungen vom System ein unterschiedlicher Antwort-Code garantiert wird.

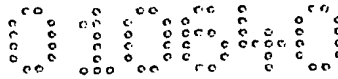
Patentanspruch 5: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1, 2 und 4 **dadurch gekennzeichnet**, dass eine geeignete Verschlüsselung einer im Vorhinein vom Sender und Empfänger vereinbarten binären Folge durch den Antwort-Code erfolgen kann, da sowohl Sender als auch Empfänger über die gleichen Informationen verfügen, wenn der Antwort-Code richtig ist.

Patentanspruch 6: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1, 2 und 3 **dadurch gekennzeichnet**, dass ein System S2, an welchem ein Anwender angemeldet sein kann, Zugang zu einem anderen System S1 haben kann, wobei in diesem Fall eine binäre Folge von S1, welche sinngemäß in analoger allgemeiner Art und Weise Bildschirmfolgen, Grafiken und Einheiten enthält, von S2 beantwortet wird.

Patentanspruch 7: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1, 2, 3 und 4 **dadurch gekennzeichnet**, dass das System die Anzahl der Bildschirmfolgen zwischen zwei Größen willkürlich verändern kann und damit die Länge des Antwort-Codes steuern kann.

Patentanspruch 8: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1 und 2 sowie die Anordnung der Eingabetasten einer speziellen Tastatur, welche vorwiegend Symbole aus einer Menge von Grafiken oder Bildern enthält, **dadurch gekennzeichnet**, dass die Grafiken oder Bilder auf der Tastatur nach logischen Gesichtspunkten (Figur 3), geordnet strukturiert sind: Spalten (S) enthalten die Formen (Kreise, Vierecke, usw.), Zeilen (Z) enthalten die Muster (kariert, gestreift, usw.) oder umgekehrt.

Patentanspruch 9: Verfahren eines graphischen Authentifizierungscodes wie in Anspruch 1, 2 und 8 **dadurch gekennzeichnet**, dass diese Anordnung auf dem Bildschirm als Eingabefeld abgebildet wird und mittels Trackball oder über einen Touch-Screen angeklickt wird.



2 Beschreibung

Stand der Technik

Technische Zugangskontrollen z.B. auf Flughäfen werden eingesetzt um autorisiertem Personal automatisiert, also unabhängig von einem Wachpersonal, den Zutritt zu Räumlichkeiten zu ermöglichen.

Eine Identifikation an einer technischen Schnittstelle ist die Identifizierung einer Person oder einer Gruppe gegenüber einem technischen System. Sie erfolgt mit Hilfe von Informationen welche dem System eine eindeutige Zuordnung zu einer Person oder Gruppe ermöglicht.

Dies kann erfolgen durch

- „Biometrische Daten“
- das Auslesen der ID Informationen einer Karte
- Eingabe einer beliebigen alphanumerischen Zeichenfolge, z.B. „Reinigung“ oder „Nov04“

Die Eingabe erfolgt über ein entsprechendes Lesegerät oder ein geeignetes Tastenfeld. Als Oberbegriff aller dieser Eingaben wird hier die Bezeichnung Code verwendet. Ist die erste Eingabe nicht personenbezogen (z.B. bei einer Karte), ist oft eine zweite Eingabe notwendig.

Nicht übertragbare Codes (Biometrische Daten)

Eine Möglichkeit die Identifikation von Berechtigten zu überprüfen ist die Personalisierung des Codes. Die Identifikation erfolgt auf der Ebene der einzelnen Personen und jeder muss zuvor am System persönlich registriert werden. In vielen Fällen ist dies aber nicht möglich z.B. bei Notfällen (Brand, Unfall, Polizeieinsatz, ...).

Die Identifikation kann erfolgen durch Ablesen des Augenhintergrunds, automatisiertes Ablesen der Fingerabdrücke, Gesichtserkennung, Stimmerkennung oder DNA. Der Überbegriff dafür ist „Biometrische Daten“.

Übertragbare Codes

Eine andere Möglichkeit der Identifikation von Berechtigten ist die Eingabe eines Codes welcher auf Wissensinformationen beruht. Personen müssen nicht persönlich dem System bekannt sein, sie müssen jedoch zuvor in den Besitz eines richtigen Codes kommen. Der Zugang kann durch einen Dritten eingerichtet werden.

Die gebräuchlichsten Codes sind

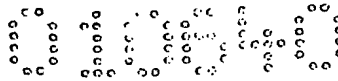
- **Zahlencode:** Dieser besteht aus einer mehrstelligen Zahl welche eingegeben wird.
- **Kartencode:** Auf einer Karte befindet sich eine Kennung. Die Karte als solche ist dabei nicht personenbezogen. Ist das Kopieren der Karte möglich, ist auch der Besitz einer „originalen“ Karte nicht Voraussetzung.
- **„Passwort“:** Dabei muss zwischen einem personenbezogenen Passwort, meist ein selbstgewähltes Wort, sowie von dem Anwender unabhängig, meist von einem Dritten vergebenen bzw. einem vorgegebenen Passwort, unterschieden werden.
- **Einmalcode:** Auf einer Liste gibt es verschiedene gültige Codes. Wenn ein Code von dieser Liste verwendet wird, ist genau dieser Code abgelaufen und kann nicht mehr verwendet werden.

Alphanumerische Zeichenfolgen können leicht von Zusehern oder Kameras erkannt werden. Der Einmalcode ist in der Handhabung umständlich und die Liste kann gestohlen werden.

Aufgabe

- Schaffung eines übertragbaren Codes auf der Basis einer Eingabe.
- Möglichkeit diesen Code in öffentlichen Bereichen auf einem speziellen Tastenfeld unabhängig von den angezeigten Symbolen oder Grafiken einzugeben, mit dem Vorteil des Einmalcodes ohne dessen Nachteile.
- Die Eingabe des Codes soll unabhängig von Sprache möglich sein.

.....
in der Einheit des Benutzers. Die Wahrscheinlichkeit der Werte soll größtmöglichst gleichverteilt sein.



Diese Eigenschaften können sein

- Farbe des Hintergrundes hinter den Eingabesymbolen
- Farbe des Eingabesymbols in der Anzeige
- Farbe der Umrahmung des Eingabesymbols (unabhängig von der Form)
- Form der Umrahmung des Eingabesymbols (unabhängig von der Farbe)
- eine Mischung aus den zuvor genannten
- usw.

Die Eigenschaften werden so gewählt, dass alle von der Tastatur angebotenen Symbole in den Sets diese in jeder Bildschirmfolge erfüllen könnten. Zu berücksichtigen ist, dass die Symbole und die Umrahmung deutlich sichtbar sind, wenn die Hintergrundfarbe mit einem der beiden übereinstimmt.

Der Antwort-Code

Der Antwort-Code besteht aus eine Menge von verschiedenen Symbolen (Bilder, Grafiken, alphanumerische Zeichen und ähnliches). Zu jedem Symbol im Antwort-Code, gibt es genau eine gleich beschriftete Taste auf der Tastatur. Einige davon werden pro Bildschirmfolge ausgewählt und zusammen mit den Verbindungseigenschaften in den Sets angezeigt. Einige Sets haben besondere Bedeutung für den Anwender, die anderen haben für die Identifikation keine Relevanz. Die Eingabe erfolgt auch bei einem Touch-Screen, wie auch bei der Verwendung eines Trackballs, niemals direkt auf den Sets des Anwenders, sondern auf eigenen angezeigten Tastenfeldern.

Je mehr Tasten (Symbole) es gibt, je mehr Sets es pro Bildschirm gibt, je öfters jedes Symbol der Tastatur in den unterschiedlichen Sets aufscheint, desto größer die Sicherheit.

Die Symbole im Antwort-Code sind kleine Grafiken mit einfacher Struktur und niedriger Komplexität. Sie müssen auf dem Bildschirm groß genug sein um einfach und schnell erfasst werden zu können und sie müssen auf einer Tastatur gut lesbar sein. Die Unterscheidungsmöglichkeit der Symbole untereinander muss für eine schnelle Unterscheidung geeignet sein.

Dabei werden die Dimensionen

- Farbe (nur wenn die Farbe keine Verbindungseigenschaft ist!)
- Form
- Muster (Struktur)

berücksichtigt.

Bei der Anzeige auf dem Bildschirm für einen Trackball oder einem Touch-Screen ist die Dimension

- Bewegung (Animation)

zusätzlich möglich. Die Verbindungseigenschaften müssen jedoch noch gut erkennbar sein.

Der Ablauf

Die Person erhält für die Identifikation folgende Informationen:

- Die Bezeichnung der zugeordneten Einheiten
- Die besonderen Grafiken welche in den Einheiten erscheinen könnten
- Die Verbindungseigenschaften zum Auffinden der richtigen Symbole
- Die Bezeichnung der zugeordneten Sets

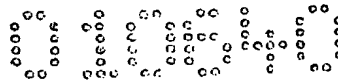
Beim Start muss entweder ein Benutzername eingegeben und an das System abgeschickt werden oder, wenn dies nicht notwendig ist, zeigt das System sofort die erste Bildschirmfolge. Bei den Grafiken sucht der Benutzer mit Hilfe der Bezeichnung seine Einheiten. Der Benutzer erkennt sofort ob in den Einheiten besondere Grafiken enthalten sind oder nicht. Mit diesem Ergebnis sind die Werte der Verbindungseigenschaft verknüpft. Mit diesen Werten findet der Benutzer in den zugeordneten Sets das richtige Symbole und drückt daraufhin die entsprechenden richtigen Tasten.

Nach der Eingabe der Informationen erscheint die nächste Bildschirmfolge oder wenn die Identifikation vollständig richtig abgeschlossen, an das Rechnersystem übermittelt und dort verifiziert ist, öffnet sich die Türe. Wurde der Code falsch eingegeben, wird eine Fehlermeldung ausgegeben und die Türe bleibt verriegelt.

Sicherheit

Der Richtwert der Anzahl der möglichen Anwender-Codes ist:

$(\text{Anz. der möglichen Einheiten} * (\text{Anz. der möglichen Grafiken in einer Einheit} \wedge \text{Anz. der zugeordneten Grafiken})) \wedge \text{Anz. der zugeordneten Einheiten} * (\text{Anz. der möglichen Sets} * (\text{Anz. der möglichen Verbindungswerte} \wedge \text{Anz. der zugeordneten Verbindungswerte})) \wedge \text{Anz. der zugeordneten Sets}$



Personenunabhängige Zugangskontrolle

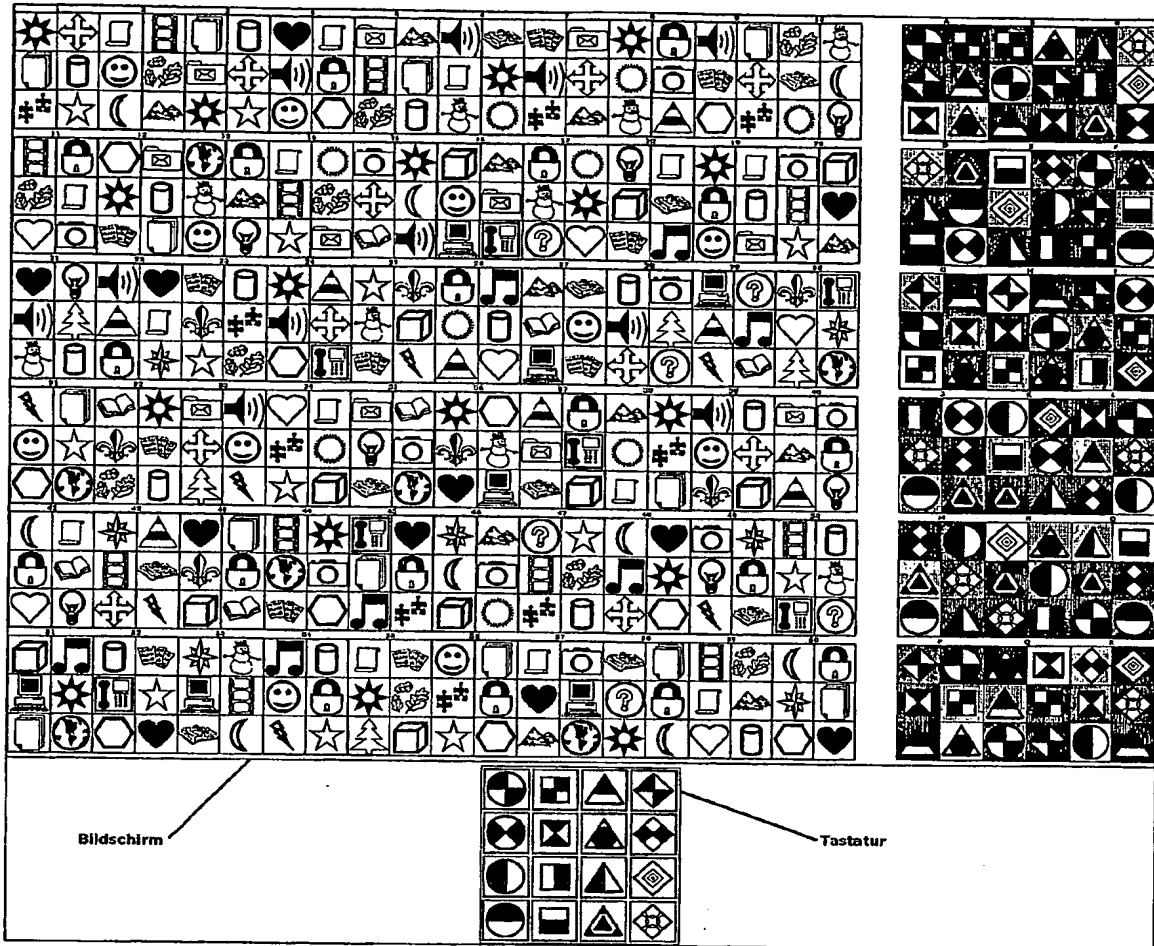
Zusammenfassung

Bei einer Passworteingabe zu einem Eingang, für einen geschützten Bereich, mit einer von einem Rechnersystem gesteuerten elektronischen Verriegelung, gibt es im öffentlichen Bereich immer das Problem der bewussten oder unbewussten Zuseher. Bei diesem graphischen Zutrittsverfahren werden diese Probleme durch die völlige Trennung von Anwender-Code (Informationen des Anwenders) und Antwort-Code (Informationen zur Verifikation) gelöst.

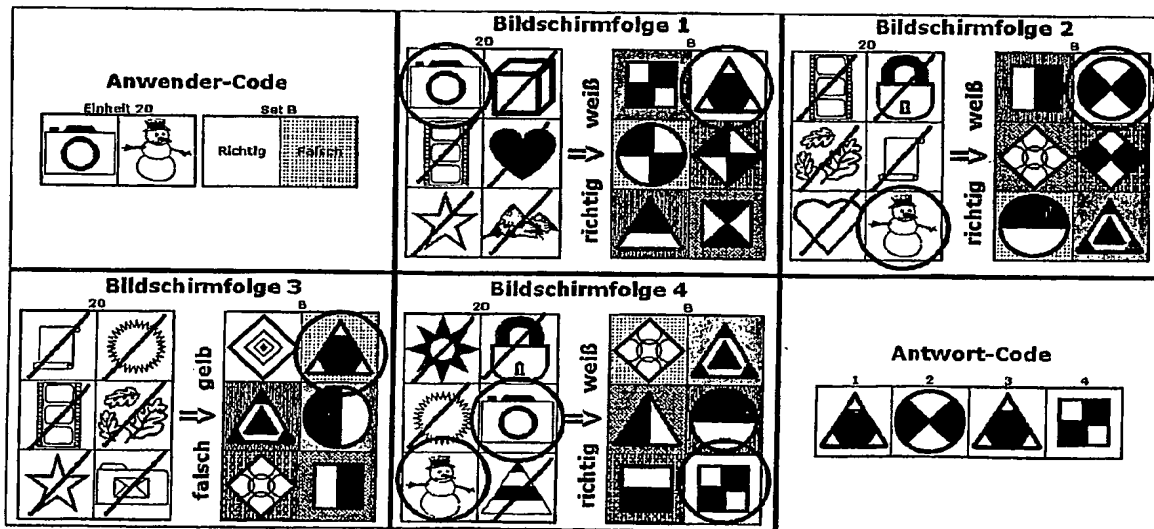
Das System übermittelt an den Anwender verschiedene graphische Bildschirmfolgen, welche mit Hilfe des graphischen Anwender-Codes erzeugt werden. Der Anwender setzt seinen Anwender-Code ein und erhält damit genau einen, für diesen Zugangsversuch gültigen, graphischen Antwort-Code. Der Antwort-Code ist ein Einmal-Code, dadurch erhalten Zuseher keine relevanten Informationen. Eine Berechnung des Anwender-Codes aus dem Antwort-Code ist bei entsprechender Konfiguration praktisch ausgeschlossen.

Durch die durchgängige graphische Realisierung ist das System von Sprachen unabhängig. Die Eingabe kann über spezielle Tastaturen, Touch-Screen oder mit Trackball erfolgen.

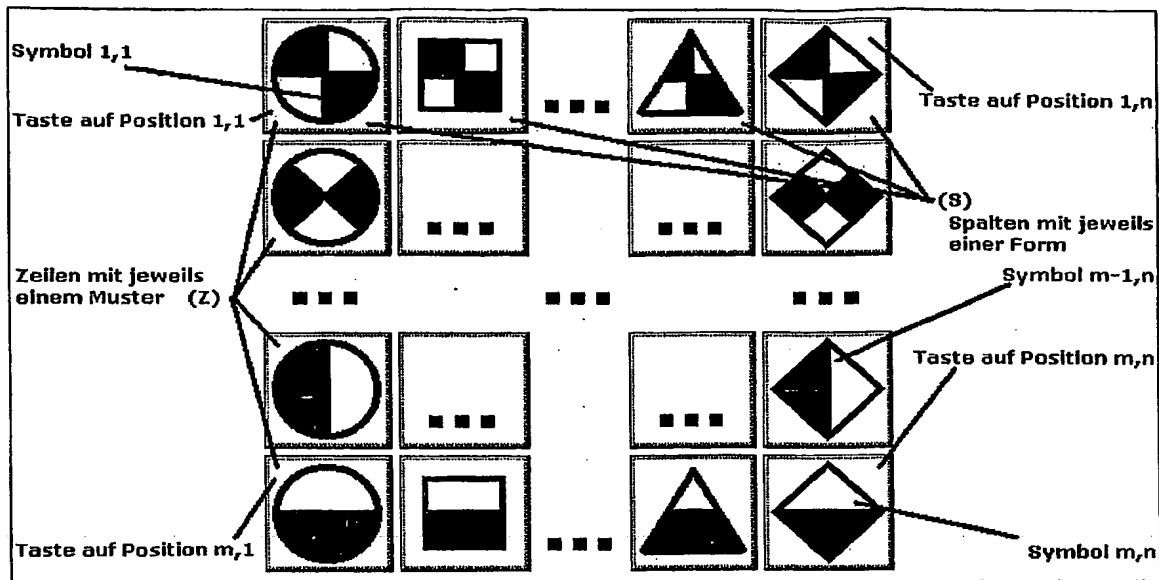
Grafik (Figur 2).



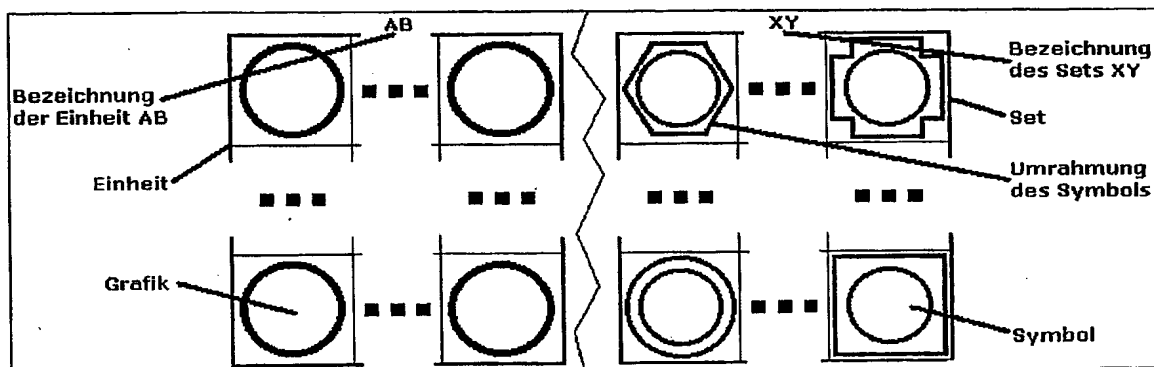
Figur 1: Bildschirm mit Tastatur



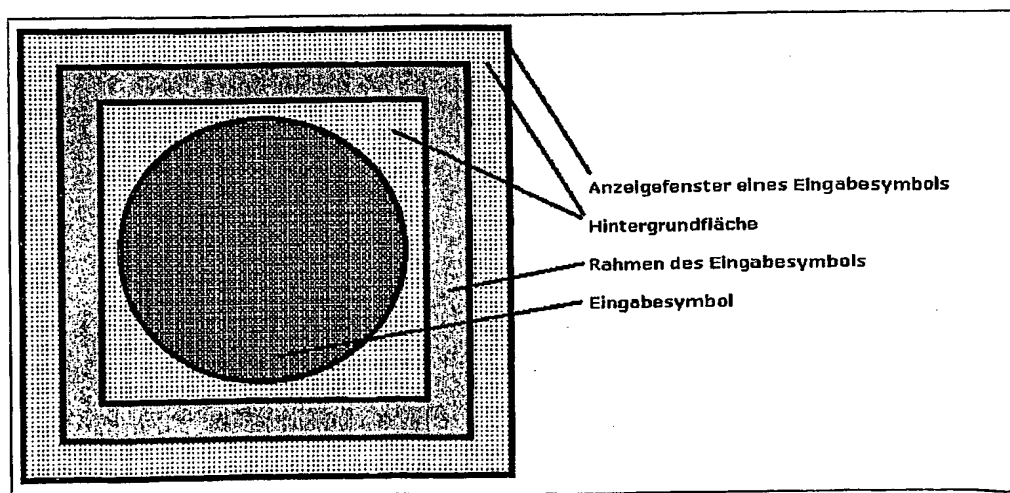
Figur 2: Beispiel mit vier Bildschirmfolgen



Figur 3: Allgemeiner strukturierter Tastaturaufbau



Figur 4: Allgemeiner Aufbau Einheit und Set



Figur 5: Allgemeiner Aufbau eines Anzeigefensters für ein Eingabesymbol